# AFFIDAVIT IN SUPPORT OF APPLICATIONS FOR SEARCH WARRANTS

I, **Patrick Steven Yaroch,** being first duly sworn, hereby depose and state as follows:

## INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for warrants for information associated with certain accounts that is stored at premises controlled by Google, located at 1600 Amphitheater Way, Mountain View, CA; and Microsoft, located at One Microsoft Way, Redmond, WA, which companies are providers of electronic communication service and remote computing services. The information to be searched is described in the following paragraphs and in Attachments A-1 and A-2. This affidavit is made in support of applications for search warrants under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703 (c)(1)(A) to require Google and Microsoft to disclose to the government copies of the information (including the content of communications) further described in Section 1 of Attachments B-1 and B-2. Upon receipt of the information described in Section 1 of Attachments B-1 and B-2, government-authorized persons will review the information to locate the items described in Section 2 of Attachments B-1 and B-2.

2. I am a Special Agent (SA) with the Federal Bureau of Investigation (FBI) and have been since May 14, 2017. Since joining the FBI in 2017, I have been assigned to a squad that investigates national security matters, including, but not limited to, counter-proliferation, counterintelligence, espionage, corporate espionage, and export compliance.

3. I have personally participated in this investigation and have witnessed many of the facts and circumstances described herein. In addition, I have received information from other federal law enforcement officials, federal government officials, and industry sources. I also have reviewed documents obtained during the course of the investigation. The statements contained in this affidavit are based on my own observations and review of documents, or reliable information provided to me by the other personnel identified above. This affidavit is being submitted for the limited purpose of obtaining search warrants. Accordingly, while this affidavit contains material information I am aware of that is pertinent to the requested search warrant, it does not include every fact known by me or other investigators concerning the investigation. Unless otherwise indicated, all written and oral statements referred to herein are set forth in substance and in part, rather that verbatim.

## PROBABLE CAUSE

### Relevant Entities and Individuals

4. Intertech Trading Corporation ("Intertech Corporation") was founded in 1990 in Atkinson, New Hampshire. Intertech Corporation is a self-described supplier of analytical instruments and mineral processing projects to Central Europe, Russia, and other Commonwealth of Independent States (CIS) countries with "12 wholly owned offices in CIS countries."

5. Intertech Instruments, LLC ("Intertech Instruments") is believed to be a Moscow-based subsidiary of Intertech Corporation. Intertech Instruments was founded by ICE Logistics, LLC of Poland.

6. Laboratory Systems and Technology ("LST") is believed to be a Moscow-based subsidiary of Intertech Corporation. LST is owned by Intertech Corporation employees, Julia Lazarenko and Alexander Shaforostov.

7. Matthew Grodowski ("Grodowski") is a resident of Salem, New Hampshire. Grodowski founded Intertech Corporation in 1990. Grodowski is the current owner and President of Intertech Corporation.

8. Timothy Kiernan ("Kiernan") is a resident of North Easton, Massachusetts. Kiernan is the General Manager of Intertech Corporation and has been an employee of Intertech Corporation since approximately 1990. Kiernan was a part owner of ICE Logistics, LLC, until he sold his shares in June 2019. According to evidence retrieved from a previous search warrant, Kiernan's business email is tkiernan@intertechcorp.net ("Subject Account 1"), hosted by a Microsoft Exchange Server.

9. Julia Markhlevskaya AKA Julia Mark ("Mark") is a resident of Hampstead, New Hampshire and is a dual Kazakhstan and US citizen. Mark serves as the Controller for Intertech Corporation and has been an employee of Intertech Corporation since approximately 1998.

10. Deborah Highfield ("Highfield") is a resident of East Hampstead, New Hampshire. Highfield serves as the Chief Financial Officer for Intertech Corporation and has been an employee of Intertech Corporation since approximately 1995.

11. Kalila Foster ("Foster") is a resident of Atkinson, New Hampshire. Foster is an employee of Intertech Corporation and has been since approximately 2003.

12. Sherry Gagnon ("Gagnon") is a resident of Derry, New Hampshire. Gagnon is an employee of Intertech Corporation and has been since approximately 2014. Gagnon was previously an employee of Intertech Corporation from approximately 2005-2011.

13. Julia Lazarenko ("Lazarenko") is a Russian citizen and resident. Lazarenko is an employee of Intertech Corporation, a part owner of ICE Logistics, LLC, and a part owner of LST. According to evidence retrieved from a previous search warrant, Lazarenko's business email is jvl@intertech-corp.ru ("Subject Account 2"), hosted by a Google Server.

14. Tatiana Kimstach ("Kimstach") is a Russian citizen and resident. Kimstach is an employee of Intertech Corporation. According to evidence retrieved from a previous search warrant, Kimstach's business email is tbk@intertech-corp.ru ("Subject Account 3"), hosted by a Google Server. On January 10, 2019, Kimstach, using Subject Account 3, sent an email Lazarenko via Subject Account 2 and another Intertech Corporation employee regarding Intertech Corporation business and provided the following signature block:

> *"заместитель директора по продажам*
> *ИНТЕРТЕК, Московский Офис*
> *Т. +7 495-232-42-25, 783-35-90*
> *Моб. +7 916 676-15-98*
> *tbk@intertech-corp.ru*
> *www.intertech-corp.ru"* which translates in English to:
>
> *"Deputy Director of Sales*
> *Intertech, Moscow Office*
> *T. +7 495-232-42-25, 783-35-90*
> *Mob. +7 916 676-15-98*
> *tbk@intertech-corp.ru*
> *www.intertech-corp.ru"*

15. Alexander Shaforostov ("Shaforostov") is a Russian citizen and resident. Shaforostov is an employee of Intertech Corporation, a part owner of ICE Logistics, LLC, and a part owner of LST. According to evidence retrieved from a previous search warrant, Shaforostov's business email is aas@intertech-corp.ru ("Subject Account 4"), hosted by a Google Server.

**Summary of the Applicable Laws and Regulations**

16. Under the International Emergency Economic Powers Act ("IEEPA"), 50 U.S.C. §§ 1701-1707, the President of the United States is granted authority to deal with unusual and extraordinary threats to the national security and foreign policy of the United States. The President, under IEEPA, can declare a national emergency through executive orders that have the full force and effect of law.

17. On August 17, 2001, under the authority of IEEPA, the President issued Executive Order 13222, which declared a national emergency with respect to the unrestricted access of foreign parties to U.S. goods and technologies, and continued in effect the Export Administration Regulations ("EAR"), 15 C.F.R. §§ 730-774. The President has issued annual Executive Notices extending the national emergency declared in Executive Order 13222 from the time period covered by that Executive Order through the present. *See, e.g.*, 83 Fed. Reg. 39,871 (Aug. 8, 2018).

18. On August 13, 2018, the President signed into law the National Defense Authorization Act of 2019, which includes provisions on export controls, entitled the Export

Control Reform Act of 2018 ("ECRA"), 50 U.S.C. § 4801, *et seq.*. In part, ECRA provides permanent statutory authority for the EAR and eliminates the need for the President to declare annually national emergencies pursuant to IEEPA and Executive Order 13222. For conduct that predates August 13, 2018, IEEPA is the controlling statute. For conduct occurring on or after August 13, 2018, ECRA is the controlling statute.[1]

19. The Export Administration Regulations ("EAR"), 15 C.F.R. §§ 730-774, control, among other things, the export and re-export to foreign countries of commercial items that also have a military application. The EAR places limitations on the export of those goods and technology that the Secretary of Commerce deems could make a significant contribution to the military potential of other countries, could prove detrimental to the national security of the United States, or are contrary to the foreign policy of the United States. The Department of Commerce maintains the Commerce Control List ("CCL"), which specifies the most sensitive goods and technologies subject to the EAR. Depending on the nature of the item, the destination country, the end-use, and the end-user of the item, a validated license from the Department of Commerce may be required for export.

20. For all exports valued over $2,500 or for which an export license is required for shipment outside of the United States, the U.S. seller, manufacturer, exporter, or its shipping agent is required to file detailed information with the United States Government, which enables

[1] The conduct described in this affidavit occurred both before and after ECRA became law. Consequently, both IEEPA and ECRA apply.

the government "to prevent the export of certain items to unauthorized destinations and/or end users." 15 C.F.R. § 30.1(b). This information is submitted electronically by filing Electronic Export Information ("EEI") in the Automated Export System ("AES") with the United States government. EEI includes, among other things, detailed information about the seller, manufacturer, or exporter; the date of export; the ultimate end-user; the country of ultimate destination; the value of the goods being exported; the Export Control Classification Number ("ECCN"); and if applicable, the export license number. By filing this information with the United States Government, the filer is certifying that the EEI information is true, accurate, and complete. 15 C.F.R. § 758.1(f). Knowingly providing false or misleading information, or causing such information to be provided, in connection with the preparation and submission of "export control documents," including EEI filings, is a violation of the EAR. 15 C.F.R. §764.2(g)(1)(ii)), IEEPA, 13 U.S.C. § 305, and 18 U.S.C. §1001; *see* 15 C.F.R. § 772.1 (EAR defines an "Export control document" to include, among other things, "EEI on the Automated Export System (AES) presented in connection with shipments to any country"). Similarly, concealing information from the Department of Commerce or U.S. Customs Service by failing to file EEI in connection with an export also violates the EAR, 13 U.S.C. § 305 and 18 U.S.C. § 1001(a)(1). *See* 15 C.F.R. § 764.2(g)(1).

21. Pursuant to Part 762 of the EAR (15 C.F.R. § 762), all companies that export any U.S. origin goods or technology outside the United States are required to maintain records of those exports for a period of five years (from the date of export or any known re-export, transshipment, or diversion of such items). As a result, exporters are required to maintain export

control documents, including EEI filings, correspondence, contracts, and financial records relating to all "exports of commodities, software, or technology from the United States and any known re-exports, transshipment, or diversions of items exported from the United States." 15 C.F.R. § 762.1.

22. Based on my training and experience, I know that individuals and businesses who engage in export conduct often retain export control documents for greater than five years for a variety of reasons, including identifying past customers and vendors, keeping track of business deals, monitoring payments, debts, and expenses, resolving business disputes, preparing tax returns, and other purposes. I also know that these records are often stored electronically on their computers for future reference and inspection.

23. Under both IEEPA and ECRA, it is a crime to willfully violate, attempt to violate, conspire to violate, or cause a violation of any order, license, regulation, or prohibition issued pursuant to the statute. 50 U.S.C. §§ 1705(a), 4819(a)(1). Willful violations of the EAR constitute criminal offenses under both IEEPA and ECRA, and shall be fined up to $1,000,000, imprisoned for up to 20 years, or both. 50 U.S.C. §§ 1705(c), 4819(b).

24. In addition to the criminal penalties imposed by the ECRA and IEEPA, Section 554 of Title 18 of the United States Code makes it illegal for anyone to fraudulently or knowingly export or send from the United States, or attempt to export or send from the United States, any merchandise, article, or object contrary to any law or regulation of the United States, or receive, conceal, buy, sell, or in any manner facilitate the transportation, concealment, or sale of such merchandise, article or object, prior to exportation, knowing the same to be intended for

exportation contrary to any law or regulation of the United States. Violations of § 554 are punishable by up to 10 years in prison, by a fine, or both. See 18 U.S.C. § 554.

25. Separately, Section 1001(a) of Title 18 of the United States Code makes it a crime for any person "in any matter within the jurisdiction of the executive, legislative, or judicial branch of the Government of the United States," knowingly and willfully to falsify, conceal, or cover up by any trick, scheme or device a material fact; to make any materially false, fictitious or fraudulent statement or representation; or to make or use any false writing or document knowing that it contains any materially false, fictitious, or fraudulent statement or entry. 18 U.S.C. § 1001(a)(1)–(3).

***Office of Foreign Assets Control (OFAC) List of Specially Designated Nationals and Blocked Persons (SDN List)***

26. The OFAC of the US Department of the Treasury administers and enforces economic and trade sanctions based on US foreign policy and national security goals against targeted foreign countries and regimes, terrorists, international narcotics traffickers, those engaged in activities related to the proliferation of weapons of mass destruction, and other threats to the national security, foreign policy or economy of the United States.

27. As part of its enforcement efforts, OFAC publishes a list of individuals and companies owned or controlled by, or acting for or on behalf of, targeted countries. It also lists individuals, groups, and entities, such as terrorists and narcotics traffickers designated under programs that are not country-specific. Collectively, such individuals and companies are called

"Specially Designated Nationals" or "SDNs." Their assets are blocked and U.S. persons are generally prohibited from dealing with them.

28. The Russian Federal Security Service ("FSB") is the principal security agency of Russia, the main internal intelligence agency, and the main successor agency to the USSR's Committee of State Security (KGB). Its main responsibilities are within the country and include counter-intelligence, internal and border security, counter-terrorism, and surveillance as well as investigating some other types of grave crimes and federal law violations.

29. Pursuant to Executive Order 13757 dated December 28, 2016, the FSB was added to the OFAC SDN List, effective December 29, 2016.

**Probable Cause to Believe that a Federal Crime was Committed**

30. As set forth below, there is probable cause to believe that Intertech Corporation, Intertech Instruments, and LST, along with Grodowski, Kiernan, Mark, Highfield, Foster, Gagnon, and other Intertech Corporation, Intertech Instruments, and LST employees intentionally falsified shipping documents, avoided and circumvented export compliance regulations, and obfuscated end-users, in violation of federal law, specifically, 18 U.S.C. § 1001(a)(1)–(3); 50 U.S.C. § 4810 et seq. – ECRA; 18 U.S.C. § 371 – Conspiracy; 50 U.S.C. §§ 1701, et seq. – IEEPA; 13 U.S.C. § 305 – Penalties for Unlawful Export Information; 18 U.S.C. § 1956 – Money Laundering; 18 U.S.C. § 1957 – Engaging in monetary transactions in property

derived from specified unlawful activity; 18 U.S.C. § 554 – Smuggling; 18 U.S.C. § 1341 – Mail Fraud; and 18 U.S.C. § 1343 – Wire Fraud ("the Offenses.")

***Intertech Instruments as Ultimate Consignee***

31. FBI examination of EEI provided by US Customs and Border Protection (CBP) revealed approximately 414 exports from Intertech Corporation identifying Intertech Instruments as the ultimate consignee between November 2002 and August 2018 for shipments of laboratory and scientific equipment, with an associated value of approximately USD$60 million.

32. According to information received from a Grand Jury subpoena, an account held by Intertech Corporation at the Bank of America received deposits totaling approximately USD$100 million between May 2011 and April 2016. Further analysis revealed Intertech Instruments was the largest single depositor during this period, with deposits totaling approximately USD$41 million. Intertech Instruments' wires referenced "payment for contract" or "payment for laboratory equipment center" on the details.

33. According to information received from additional Grand Jury subpoenas, Intertech Trading Corporation closed its account at Bank of America and as of April 2019, held four Checking accounts and one Money Market savings account with Eastern Bank. Between September 2017 and April 2019, Intertech Trading Corporation received approximately USD$23 million in incoming funds. Within this same time period, outgoing funds totaled approximately USD$21 million. Further analysis revealed that the two most significant sources of income originated from international wire transfers from Intertech Trading Corporation (foreign bank

accounts) and wire transfers from Intertech Instruments, with deposits totaling approximately USD$9.8 million and USD$5.8 million, respectively.

34. Open source business registry information identified Intertech Instruments as a wholesale distributor of commodities in several industries, including chemical agents, explosives, fuel, and precious metals. As a wholesaler distributor, Intertech Instruments is not a laboratory or other facility with an identifiable need for the equipment purchased, thus Intertech Instruments is not the ultimate consignee of these products; however, no information on the true ultimate consignees was reported by Intertech Corporation in its EEI, as required by the EAR.

***Examples of Failing to Identify the Ultimate Consignee: Sales to the Federal Security Service (FSB)***

35. Evidence obtained during the course of the investigation indicates that Intertech Corporation failed to identify the Ultimate Consignee in its export filings. Specifically, email, financial, and export records maintained by Intertech Corporation identified at least four transactions completed with the FSB between March 2015 and September 2016. According to DOC and CBP records, during that same period, no EEI filings identified the FSB as a consignee, in violation of the EAR. These transactions are detailed below:

a. Intertech Instruments Purchase Order 2065

i. Dated March 27, 2015

ii. EEI Listed Ultimate Consignee: Intertech Instruments

iii. Actual End User: Institute of Criminalistics FSB RF

iv. Value: $1,532.00

v. An email sent on March 26, 2015, from Lazarenko sent via Subject Account 2 to Kiernan, using Subject Account 1, and two other Intertech Corporation employees, contained nine attachments related to the above order. The attachments include the Purchase Order, Coversheet, and various end user forms for Purchase Order 2065.

b. Intertech Instruments Purchase Order 2133

i. Dated August 12, 2015

ii. EEI Listed Ultimate Consignee: Intertech Instruments

iii. Actual End User: Federal Security Service, SPb department

iv. Value: $8,064.00

v. An email sent on August 18, 2015, from Lazarenko, sent via Subject Account 2, to two Intertech Corporation employees, contained attachments related to multiple orders, including the Purchase Order and Coversheet for Purchase Order 2133.

c. Intertech Instruments Purchase Order 2154

i. Dated September 11, 2015

ii. EEI Listed Ultimate Consignee: Intertech Instruments

iii. Actual End User: Federal Service of Security of Russia

iv. Value: $9,430.00

v. An email sent on September 10, 2015, from Lazarenko, sent via Subject Account 2, to Kiernan, using Subject Account 1, and two other Intertech Corporation employees, contained five attachments related to the above order. The attachments include the Purchase Order, Coversheet, and various end user forms for Purchase Order 2154.

d. Intertech Instruments Purchase Order 2327

i. Dated September 7, 2016

ii. EEI Listed Ultimate Consignee: Intertech Instruments

iii. Actual End user: Institut Kriminalistiki FSB (Criminalistics Institute of FSB special equipment center)

iv. Value: $20,498.94

36. On December 20, 2017, Kiernan joined a conference call with multiple employees of Thermo Fisher Scientific. Kiernan indicated that he was worried about future sanctions targeting the FSB. Kiernan stated that if the FSB is subject to sanctions, big orders will go away. He continued by stating that FSB business brings some good projects every year or every other year, quantifying it to a quarter to a third of Intertech Corporation's vibrational business. He further added that the FSB controls the larger federal forensic labs.

37. According to an interview of Kiernan in June 2019, Kimstach worked in an FSB lab many years ago, maintains some of those connections, and works closely with the FSB for her current sales.

***DOC BIS Is Informed Letter***

38. On September 10, 2018, BIS and FBI served Intertech Corporation with an "Is Informed Letter" notifying Intertech Corporation of new imposed license requirements. The Is Informed Letter contained the following text:

39. *"The Bureau of Industry and Security (BIS), U.S. Department of Commerce is charged with administering and enforcing the Export Administration Regulations (EAR) (15 C.F.R. Parts 730 -774). Section 744.4(a) of the EAR imposes a licensing requirement on the export, reexport, or transfer (in-country) of any item subject to the EAR if the exporter or reexporter has knowledge that the item may be used, directly or indirectly, in the design, development, production, stockpiling, or use of chemical or biological weapons in or by any country or destination, worldwide. Furthermore, Section 744.4(b) of the EAR provides that BIS may inform exporters (in-country) of any item subject to the EAR to a specified end user because there is an unacceptable risk of use in or diversion to such activities."*

40. *"This Letter informs [Intertech Corporation] that a license is required for the export, reexport, or transfer (in-country) of any laboratory or scientific equipment or materials to Intertech Instruments in Moscow, Russia. When submitting a license application for such exports or reexports, you must indicate in the 'Additional Information' box that the application is submitted based on a risk of diversion to chemical or biological end uses in accordance with Section 744.4(b) of the EAR."*

41. *"Such export license applications will be reviewed in accordance with the license review standards set forth in Section 744.4(d) of the EAR."*

42. After receiving the Is Informed Letter, Intertech Corporation changed its business practices to circumvent and evade the requirements set forth by the Is Informed Letter. The following conversations demonstrate this intent:

43. On October 16, 2018, Highfield and Gagnon had the following conversation via telephone:

a. Gagnon *"Like, hypothetically if somebody audits, like, all of those orders would still reference Intertech Instruments unless he wants us to like go in and redo all of the orders that are canceled to say Intertech Instruments and rename 'em. Do you know what I mean?"*

*b.* Highfield – *"How do they rename them, like, what do they use for a name now? Is it like one name for all of them and just different PO Numbers?"*

c. Gagnon – *"Well, no, they are keeping... it just says the following orders will be placed and shipped by MASHPROM Exports together, so it's like basically just renaming Intertech Instruments Consol. with MASHPROM Exports."*

d. Highfield – *"So couldn't we just add MASHPROM and keep everything like on like the name of the contract and not have to change anything else?"*

*e.* Gagnon – *"Right but the whole point is that like we would still, if we didn't delete Intertech Instruments because technically they have a cancellation letter saying that they didn't buy that from us. So on our end, like, if we don't delete Intertech Instruments from those POs and we just add Mashprom Exports to the name like*

*Intertech Instruments there is still the reference there. Do you know what I'm saying?"*

f. Highfield – *"Mmhmm"*

g. Gagnon – *"I guess this is gonna be a Tim [Kiernan] question. I mean what are the chances that anybody would look at our internal stuff?"*

*h.* Highfield – *"Well, well, I would venture to say good but, you know."*

*i.* Gagnon – *"Well I bet he didn't think the FBI was going to come in and ask for his name either so at this point I just feel like we should probably cover our butts, you know?"*

*j.* Highfield – *"I know but that does mean quite a bit of work, you know, if you are going to cancel all of those and redo the purchase orders and rename them."*

*k. Gagnon – "No, No, No. I don't necessarily mean like redo, oh yeah, so, no because we don't put Intertech Instruments on the PO's so it would be more like umm."*

l. Highfield – *"You do for a reference"*

*m.* Gagnon – *"Well I put PO. I don't put the words Intertech Instruments"*

*n. Highfield – "So does Mashprom still have a PO number too? Is it the same PO number?"*

o. Gagnon – *"I don't know if she actually sent me something that says... I still have to ask Julia Mark."*

44. On January 16, 2019, Highfield and Mark called Kiernan to discuss order changes and combining orders as per Lazarenko's requests. Highfield stated that she was having problems trying to match numbers and though the Prime [Prime SIA] ones come from Prime, she believed they were Intertech Instrument orders. Kiernan stated that Julia Lazarenko can't be mixing up money between MPE and Intertech Instruments.

45. On January 16, 2019, Lazarenko called Kiernan and Kiernan asked "*about, you know, these constant changing of paperwork and then some of these payments coming in.*"

*a.* Lazarenko - "*What payments?*"

*b.* Kiernan – "*Well payments from Prime, and, you know, they're telling me that a payment from Prime was applied to an Intertech Instruments contract?*"

c. Lazarenko – "*Yes.*"

d. Kiernan – "*Alright, in the future we can't have that.*"

e. Lazarenko explains this was a complicated case involving direct shipping from Riga to Intertech Instruments before the new year.

f. Kiernan – "*If we ever get audited on this exchange thing that we have going on, it's gonna complicate us. It's gonna complicate explanations because I.. you know, we can't do this.*"

g. …

h. Lazarenko – "*next week we will have bank account for the new company and will do it only through the new company.*"

46. On January 17, 2019, Highfield called Kiernan to talk about emails regarding shipments. Highfield said, *"I'm not sure you want all these things being emailed."* Later on in the conversation, Highfield stated *"it's saying right in the email, we're changing the Intertech Instrument order to the.."* Kiernan interjected *"Well it's not, I mean, its got to be changed back to this Prime and whatever, Intertech Instruments shouldn't be involved… by doing that, it's not any conflict with the Is Informed Letter."*

47. On January 18, 2019, Mark called Foster to talk about MPE (Mashprom Export LLC) shipments for Moscow. Mark said *"you know like, they are interchanging Intertech Instruments with MPE*." Later Mark continued *"MPE didn't exist before export license problem."* Finally Mark stated *"We will not be applying much anymore, we will not, because most of them will be diverted to MPE, like they already started, right. And then when Julia [Lazarenko] gets her new company, called Laboratory Systems, then it will be through them. So Intertech Instruments will continue shipping only non-US exports, all US will be diverted."*

48. On January 23, 2019, Lazarenko called Kiernan to discuss business matters. Kiernan explained to Lazarenko that *"Debbie [Highfield] is getting, I guess, concerned about the, the wording in some of these emails, we really don't want to put in emails. Especially, simply our ability to change Intertech Instruments orders to Prime [SIA] orders and things along that line."*

***Creation of LST***

49. On November 4, 2018, Kimstach sent an email via Subject Account 3, to Kiernan, Lazarenko, and Shaforostov, utilizing Subject Accounts 1, 2, and 4 respectively, with the subject line: forensic iS50. The body of the email contained the following text *"To All: Me most concern is forensic project (iS50) If iS50 will be not delivery in time – it means to break President's program of financing of Moscow forensic labs in this year If we NOT deliver before Nov 30 we may get EFFECTS 1) Lost $100 000 (contract warranty amount) 2) Intertech Instruments in 'Black List' 3) Personal sanction (unpleasant effects:..) against Tim Kiernan and M. Grodowski (very possible!) – the Buyer DID check all high persons in Intertech Instruments and Intertech Corp 4) Unpleasant issues for Andrei Dmitrievski as Director 5) Complete closing of business of Instruments with unpleasant effects for officials and owners 6) Me (change business and change mobile tel number etc –to disappear from this business) Such are people from the other side ::::. (they have 'very long hands' – believe me) If we deliver in time (I know situation) the worst – closing business of Instruments or CAC and open new rubles companies (but very low probability) Think!!"*

50. On November 9, 2018, Shaforostov sent an email via Subject Account 4, to Kiernan and Lazarenko, utilizing Subject Accounts 1 and 2 respectively, with the subject line: UPDATE RE: New company rules and commission. The body of the email contained the following text *"Tim, Just to update you on the progress and few things that we will also need to discuss: Suggested Name: OOO << лабораторные информационные системы>> / Laboratory Information Systems Timing: registering will take up to 2 weeks. The cost of*

*auditors services and state fee for company registration: 40 000 RUR We have evaluated Legal address options: a. Outside location 17 000 RUR with the space 15 sq.m – can use as a workshop for service or small stock. It is close to my location and I can easily bring things in and out and be there if tax office will want to check. I talked to a guy, this space is still available but he is actively looking for he lease. Me and Julia agree this is the ideal option. B. 15 000 RUR – another location, but no space. Not good option in my opinion, no space just legal address… c. Allocate some space in the current office building. E.g. storage cell in the basement. This will be looking 'funny' to say the least. Also close to our current locations which presumes a connection in my opinion…. The cost is around 15 000/month for actual 7 sq.m (so it will not bring extra cost to the group as a whole). Authorised capital: a. The capital for registration purposes can be some sort of minimal value, say 100 000 RUR b. For the first months company will need some money for rents and some other costs (e.g. import taxes if first supplies are not prepaid0. In my opinion it is best to provide the starting financing from the cashbox as "shareholders loan" with the consequent return to cashbox as soon as needed profit accumulated. CEO and Accounting: a. We will need someone internally. I have preliminary talked to Durov, he seems to be OK but with same compensation as for Andrew Dmitrievsky. b. Alternatively If we agree I can be CEO with no extra payments. c. Accounting for the first period may be assisted from the current accountants. CEO and Accountant may be the same person for the first. Let us know if you have any suggestions or comments. Alex"*

51. On February 14, 2019, Kiernan sent an email via Subject Account 1 to ursula.lackner@thermofisher.com with the subject line: New Russian Company. The body of the email contained the following text, *"We needed to establish a new company in Russia because of a couple of late deliveries are placing us on some lists that do not allow us participate in tenders. The company is owned by our Moscow office Director, Alexander Shaforostov. Laboratory Sytems and Technologies (LST) LTD INN/KPP 7704470485 / 770401001 OKPO 35297568 OGRN: 5187746029895 Legal adress : Burdenko st, 14 bld A 4 stage, office 1 room 3 Moscow 119121 RUSSIA Tel : (985) 552-3669 e-mail: info@lims-consult.ru<mailto:info@lims-consult.ru> General Director Mr. A.A.Shaforostov"*

52. As of August 2019, open source business records for LST revealed the company was registered in December 2018 and owned by Lazarenko and Shaforostov, each owning 50%. Also as of August 2019, open source business records for Intertech Instruments revealed 100% ownership by ICE Logistics of Poland. As of October 2019, open source business records for ICE Logistics revealed Lazarenko and Shaforostov have each owned 50% of the company since June 2019. However, in October 2017, open source business records for ICE Logistics showed Kiernan and Lazarenko as owning 50% each. Based on my training and experience, I believe Kiernan transferred his shares of ICE Logistics to Shaforostov likely in an effort to conceal Kiernan's control of Intertech Instruments and LST.

53. Intertech Corporation employees, Lazarenko and Shaforostov, own both LST and Intertech Instruments, via ownership of the holding company. According to an interview of Kiernan in June 2019, LST operates in the same office space as both Intertech Instruments and

Intertech Corporation. Based on my training and experience, and considering the shared ownership, shared office space, and the dates of issuance of the Is Informed letter and the registration of LST, I believe Intertech Instruments to be doing business as LST for the purposes of circumventing the licensing requirements imposed by the Is Informed letter.

***Knowledge of Export Compliance Regulations***

54. On Friday, June 15, 2012, Kiernan, via Subject Account 1, sent an email to multiple recipients, including Kimstach, via Subject Account 3, and Shaforostov, via Subject Account 4, with the subject line: *Memo on Export Compliance.* The email contained three attachments which combined to form Intertech Corporation's first formal Export Compliance Policy. One attachment, titled *Export Compliance Policy 2012 rev01,* contained the following text:

55. *"you need a completed end-user statement (BIS form 711) (same as before in Russian ) that clearly indicates all parties involved. The end-user statement should also identify the end-use or application intended for the product to be exported."*

56. On Thursday, January 15, 2015, Kiernan, using Subject Account 1, sent an email to representatives of each Intertech Office, including Lazarenko, using Subject Account 2, with an updated Sales and Marketing Memo regarding export compliance, and an updated BIS 711 form attached. The email contained the following text: "*End-Use/Application: as some of you might be aware, we currently have a shipment that was seized by US Customs in Boston. It*

*seems that the shipment was seized due to the fact that we did not provide adequate information on the end-use/application. It is critical that we start receiving this information.*"

57. On Tuesday, January 21, 2015, Gagnon sent an email to Foster and a former Intertech Corporation employee. Within the email, Gagnon provided the definitions of Ultimate and Intermediate consignees as follows: "***Ultimate consignee.*** *The principal party in interest located abroad who receives the exported or reexported items. The ultimate consignee is not a forwarding agent or other intermediary, but may be the end-user.* ***Intermediate consignee.*** *The person that acts as an agent for a principal party in interest for the purpose of effecting delivery of items to the ultimate consignee. The intermediate consignee may be a bank, forwarding agent, or other person who acts as an agent for a principal party in interest. The intermediate consignee is the party in a foreign country who receives and then delivers the merchandise to the ultimate consignee. The city and country are only needed for the address. If a validated export license is required the intermediate consignee must be the same as designated on the license."*

58. On Tuesday, July 26, 2016, Kiernan, using Subject Account 1, sent an email to Lazarenko, via Subject Account 2, and two other Intertech Corporation employees, regarding the necessity of the BIS-711 form. Within the body of the email, Kiernan states "*We also need to protect ourselves legally. If we get audited by Homeland Security or US Dept. of Commerce, we need to prove that we know who the end user is and what they are doing with our equipment."*

59. On Tuesday, June 20, 2017, Kiernan sent an email to the multiple recipients, including Shaforostov, via Subject Account 4, which contained an updated Export Compliance Policy Manual and an appendix of current export compliance forms including: BIS-711 End

User Form, Chemical and Biological Weapons screen checklist, Diversion risk checklist, Missile screen checklist, Nuclear screen checklist, Statement of Ownership, general end user statement, manufacturer specific end user statements, Russia Sanctions 2 form, Non Nuclear End Use Certification, and a Verification Statement.

60. In addition, on March 19, 2018, Mark called Lazarenko to discuss orders. Lazarenko told Mark that she spoke to Kiernan about switching the two Spectrometers. According to Lazarenko, Kiernan said that he would pretend he doesn't know about it if done in a non-official way. Mark didn't understand what that meant. Lazarenko said: "*That means that you guys will register them the way you want in your books and we, on our end, can send it to whomever we want.*" Mark asked why it should be done that way. Lazarenko said: per Kiernan it takes too long, that's why. Based on my training and experience, I believe this conversation demonstrates that certain members of Intertech Corporation's management knew the proper ways to file export documents under the EAR, yet intentionally chose not to.

**Probable Cause to Believe that the Target Accounts Contain Evidence, Fruits, and Instrumentalities**

61. I also have probable cause to believe that the Target Accounts, as listed in Attachments A-1 and A-2, contain evidence, fruits, and instrumentalities of the crimes identified above, as described in Attachments B-1 and B-2. In my training and experience, I have learned that Google or Micorsoft ("the Providers") provide a variety of on-line services, including electronic mail ("email") access to the public and to companies. The Providers allow subscribers

to obtain email accounts at custom domains, like the email accounts listed in Attachments A-1 and A-2. Subscribers often obtain an account by registering with a provider. During the registration process for custom domains, the provider asks the subscriber to provide basic personal and financial information. Therefore, the computers of the Providers are likely to contain stored electronic communications (including retrieved and un-retrieved email for subscribers) and information concerning subscribers and their use of the Provider's services. Based on my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

62. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber's full name, physical address, telephone numbers, and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and experience, I know that, even if subscribers insert false information to conceal their identity, this information often provides clues to their identity, location, or illicit activities.

63. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can included the date on which the account was created, the length of service, records of log-in (i.e. session) times and durations, the types of service utilized, the status of the

account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocal address ("IP address") used to register the account and the IP addresses associated with a particular login to the account. Because every device that connects to the internet must use an IP address, IP address information can help identify which computers or other devices were used to access the email account.

64. In my training and experience, in some cases email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any action taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

65. As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, when, where, why, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of

occupancy" while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the IP addresses from which users access the email account, along with the date and time of that access. By determining the physical location associated with the logged IP address, investigators can understand the chronological and geographic context of the email account access and use relating to the crimes under investigation. This geographic and timeline information may tend to either inculpate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (e.g. location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the crimes under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (e.g. communications relating to the crime), or consciousness of guilt (e.g. deleting communications in an effort to conceal them from law enforcement).

## CONCLUSION

66. Based on the foregoing, I request that the Court issue the proposed search warrants. Because the warrants will be served on Google and Microsoft, which will then compile

the requested records at a time convenient to those entities, reasonable cause exists to permit the execution of the requested warrants at any time in the day or night.

Respectfully submitted,

/s/ Patrick Steven Yaroch
Patrick Steven Yaroch
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me
on January 14, 2020:

Andrea K. Johnstone
UNITED STATES MAGISTRATE JUDGE

**ATTACHMENT A-1**

*Property to be searched*

This warrant applies to information associated with tkiernan@intertechcorp.net that is stored at premises owned, maintained, controlled, or operated by Microsoft, a company headquartered at One Microsoft Way, Redmond, WA.

**ATTACHMENT B-1**

*Particular things to be seized*

1. **Information to be disclosed by Microsoft (the "Provider")**

To the extent that the information described in Attachment A-1 is within the possession, custody, or control of the Provider, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to the Provider or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is requested to disclose the following information to the government for each account or identifier listed in Attachment A-1:

a. The contents of all emails to and from each account listed in Attachment A-1, from January 2015 through the present, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;

b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. The types of service utilized;

d. All records or other information stored by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files; and

e. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken.

The Provider is hereby ordered to disclose the above information to the government within 14 days of service of this warrant.

2. **Information to be seized by the government**

All information described above in Section 1 that constitutes evidence of violations of 18 U.S.C. § 1001(a)(1)–(3); 50 U.S.C. § 4810 et seq. – ECRA; 18 U.S.C. § 371 – Conspiracy; 50 U.S.C. §§ 1701, et seq. – IEEPA; 13 U.S.C. § 305 – Penalties for Unlawful Export Information; 18 U.S.C. § 1956 – Money Laundering; 18 U.S.C. § 1957 – Engaging in monetary transactions in property derived from specified unlawful activity; 18 U.S.C. § 554 – Smuggling; 18 U.S.C. § 1341 – Mail Fraud; and 18 U.S.C. § 1343 – Wire Fraud, those violations involving Intertech Corporation, Intertech Instruments, and/or LST, and occurring after January 2015, including, for each account or identifier listed on Attachment A-1, information pertaining to the following matters:

a. All communications, records, and files relating to the possible identification, procurement, purchase, preparation, packaging, description, valuation, invoicing,

licensing, concealment, sale, supply, transportation, exportation, shipment, or trans-shipment of goods from the United States or other countries to Russia and involving either Intertech Instruments or LST, including communications relating to payments and receipt of payments for said transactions;

b. All communications, records, and files pertaining to the obfuscation of end-users to the United States Government.

c. Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crimes under investigation and to the email account owners;

d. Evidence indicating the email account owner's state of mind as it relates to the crimes under investigation;

e. The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s);

f. The identity of the person(s) who communicated with the user ID about matters relating to the crimes under investigation including records that help reveal their whereabouts.